



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/609,261	06/26/2003	Ramarathnam Venkatesan	MSI-1042US	8089
22801	7590	04/05/2007	EXAMINER	
LEE & HAYES PLLC			POLTORAK, PIOTR	
421 W RIVERSIDE AVENUE SUITE 500				
SPOKANE, WA 99201			ART UNIT	PAPER NUMBER
				2134

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/05/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/05/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)
	10/609,261	VENKATESAN ET AL.
	Examiner Peter Poltorak	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 26 June 2003.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-20 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>06/26/03</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 have been examined.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6, 8-18, 20-29, 31-40 and 42-47 U.S. Patent Application No. 10/609260. Although the conflicting claims are not identical, they either recite a concomitance of the claim features, or they are their obvious modifications.

For example, compare claims 1-4(10609260) with claims 1-2 of the current application (10609261).

Claim Objections

3. Claims 2, 4, 9, 11, 16 and 18 are objected to because of the following informalities:

the claims are incomplete. Applicant should identify in the claim language the

meaning of "*" or " \leftarrow " (e.g. see claim 11: $x \notin Z_p$).

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The claimed invention is directed to non-statutory subject matter. Claims 1, 8 and 15 with their dependent claims are directed to a method and an apparatus performing some arithmetic calculation. However, these calculations, as recited in the claim language, do not produce a useful, tangible result. In particular, claims 1, 8 and 15 do not recite any useful, even if abstract (such as a signature) result and there is no tangible result, e.g. transferring a signature to another entity.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-3, 8-10 and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boldyreva ("Efficient threshold signature, multisignature and blind

signature schemes based on the Gap-Diffie-Hellman-group signature scheme, 2002).

Boldyreva discusses blind signatures using Gap-Diffie-Hellman (GDH) group of elements (e.g. "Abstract").

5. As per claim 1, Boldyreva discloses receiving first data to be blindly signed; establishing parameter data for use with signature generating logic that encrypts data, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman group of elements relating to said curve; determining private key data and corresponding public key data using said signature generating logic; and generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature (e.g. "The blind GDH signature scheme, pg. 12).
6. Boldyreva discussion of blind GDH signatures also reads on claims 2-7.
7. Although, Boldyreva does not explicitly disclose encrypting data based on a Jacobian of at least one curve, the examiner points out that the choice of encrypting data based on a Jacobian of at least one curve, would have been obvious to one of ordinary skill in the art given that they are well known (e.g. Zhand on pg. 7) and barring any unexpected results.
8. As per claims 8 and 15, Boldyreva does not explicitly teach computer readable medium and memory used in the data signing.

Zhand discloses real life applications of blind signatures, in which the computers are utilized (Zhand, "Introduction", pg. 1-2), and computers use memory to compute

code stored on a readable medium. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize computers (that comprise computer readable medium and memory). One of ordinary skill in the art would have been motivated to perform such a modification in order to provide anonymity of users in electronic applications, such as electronic voiding and payment system. Furthermore, the examiner points out that an ordinary artisan would readily recognize the value of computers (with memory and readable medium for storing computer code) given the benefit of the inherent nature of computers to compute data.

9. Claims 9-14 and 16-20 are substantially equivalent to claims 2-7; therefore claim 9-14 and 16-20 are similarly rejected.

Conclusion

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-

3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



3/30/07



KAMBIZ ZAND
PRIMARY EXAMINER